UNIVERSAL COUNTING OF LATTICE POINTS IN POLYTOPES

Imre Bárány[1]
Mathematical Institute of the Hungarian Academy of Sciences,
POB 127, 1364 Budapest, Hungary
barany@math-inst.hu, and
Dept. Mathematics,
University College London,
Gower Street, WC1E 6BT London, UK

Jean–Michel Kantor
Institut Mathématique de Jussieu,
Université Paris 7, 4 Place Jussieu,
75252 Paris, France
kantor@math.jussieu.fr

Abstract. Given a lattice polytope P (with underlying lattice $\mathbb{L}$), the universal counting function $\mathcal{U}_P(\mathbb{L}') = |P \cap \mathbb{L}'|$ is defined on all lattices $\mathbb{L}'$ containing $\mathbb{L}$. Motivated by questions concerning lattice polytopes and the Ehrhart polynomial, we study the equation $\mathcal{U}_P = \mathcal{U}_Q$.

Mathematics Subject Classification: 52B20, 52A27, 11P21

[1]Partially supported by Hungarian Science Foundation Grant T 016391, and by the French–Hungarian Bilateral Project Balaton F–30/96

1. The universal counting function

We will denote by V a vector space of dimension n, by $\mathbb{L}$ a lattice in V, of rank n. Let

$$\mathcal{G}_{\mathbb{L}} = \mathbb{L} \rtimes GL(\mathbb{L})$$

be the group of affine maps of V inducing isomorphism of V and $\mathbb{L}$ into itself; in case

$$\mathbb{L} = \mathbb{Z}^n \subset V = \mathbb{Q}^n, \mathcal{G}_n = \mathbb{Z}^n \rtimes GL(\mathbb{Z}^n)$$

corresponds to affine unimodular maps. An $\mathbb{L}$–polytope is the convex hull of finitely many points from $\mathbb{L}$; $\mathcal{P}_{\mathbb{L}}$ denotes the set of all $\mathbb{L}$–polytopes. For a finite set A denote by $|A|$ its cardinality. Finally, let $\mathcal{M}_{\mathbb{L}}$ be the set of all lattices containing $\mathbb{L}$.

Definition 1. Given any $\mathbb{L}$–polytope P, the function $\mathcal{U}_P : \mathcal{M}_{\mathbb{L}} \to \mathbb{Z}$ defined by

$$\mathcal{U}_P(\mathbb{L}') = |P \cap \mathbb{L}'|$$

is called the *universal counting function* of P.

This is just the restriction of another function $\mathcal{U} : \mathcal{P}_{\mathbb{L}} \times \mathcal{M}_{\mathbb{L}} \to \mathbb{Z}$ to a fixed $P \in \mathcal{P}_{\mathbb{L}}$, where $\mathcal{U}$ is given by

$$\mathcal{U}(P, \mathbb{L}') = |P \cap \mathbb{L}'|.$$

Note, further, that $\mathcal{U}_P$ is invariant under the group, $\mathcal{G}_{tr}$, generated by $\mathbb{L}$–translations and the reflection with respect to the origin, but, of course, not invariant under $\mathcal{G}_{\mathbb{L}}$.

Example 1. Take for $\mathbb{L}'$ the lattices $\mathbb{L}_k = \frac{1}{k}\mathbb{L}$ with $k \in \mathbb{N}$. Then

$$\mathcal{U}_P(\mathbb{L}_k) = |P \cap \frac{1}{k}\mathbb{L}| = |kP \cap \mathbb{L}| = E_P(k)$$

where E_P is the Ehrhart polynomial of P (see [Ehr]). We will need some of its properties that are described in the following theorem (see for instance

[Ehr],[GW]). Just one more piece of notation: if F is a facet of P and H is the affine hull of F, then the relative volume volume of F is defined as

$$\mathrm{rvol}(F) = \frac{\mathrm{Vol}_{n-1}(F)}{\mathrm{Vol}_{n-1}(D)}$$

where D is the fundamental parallelotope of the $(n-1)$–dimensional sublattice of $H \cap \mathbb{L}$. For a face F of P that is at most $(n-2)$–dimensional let $\mathrm{rvol}(F) = 0$. Note that the relative volume is invariant under $\mathcal{G}_{\mathbb{L}}$ and can be computed, when $\mathbb{L} = \mathbb{Z}^n$, since then the denominator is the euclidean length of the (unique) primitive outer normal to F (when F is a facet).

Theorem 1. *Assume P is an n–dimensional $\mathbb{L}$–polytope. Then E_P is a polynomial in k of degree n. Its main coefficient is* $\mathrm{Vol}(P)$*, and its second coefficient equals*

$$\frac{1}{2} \sum_{F \text{ a facet of } P} \mathrm{rvol}(F).$$

It is also known that E_P is a $\mathcal{G}_{\mathbb{L}}$–invariant valuation, (for the definitions see [GW] or [McM]). The importance of E_P is reflected in the following statement from [BK]. For a $\mathcal{G}_{\mathbb{L}}$–invariant valuation ϕ from $\mathcal{P}_{\mathbb{L}}$ to an abelian group G, there exists a unique $\gamma = (\gamma_i)_{i=0,\ldots,n}$ with $\gamma_i \in G$ such that

$$\phi(P) = \sum \gamma_i e_{P,i}$$

where $e_{P,i}$ is the coefficient of k^i of the Ehrhart polynomial.

It is known that E_P does not determine P, even within $\mathcal{G}_{\mathbb{L}}$ equivalence. [Ka] gives examples lattice–free $\mathbb{L}$–simplices with identical Ehrhart polynomial that are different under $\mathcal{G}_{\mathbb{L}}$. The aim of this paper is to investigate whether and to what extent the universal counting function determines P.

We give another description of $\mathcal{U}_P$. Let $\pi\colon V \to V$ be any isomorphism satisfying $\pi(\mathbb{L}) \subset \mathbb{L}$. Define, with a slight abuse of notation,

$$\mathcal{U}_P(\pi) = |\pi(P) \cap \mathbb{L}| = |P \cap \pi^{-1}(\mathbb{L})|.$$

Set $\mathbb{L}' = \pi^{-1}(\mathbb{L})$. Since $\mathbb{L}'$ is a lattice containing $\mathbb{L}$ we clearly have

$$\mathcal{U}_P(\pi) = \mathcal{U}_P(\mathbb{L}').$$

Conversely, given a lattice $\mathbb{L}' \in \mathcal{M}_{\mathbb{L}}$, there is an isomorphism π satisfying the last equality. (Any linear π mapping a basis of $\mathbb{L}$ to a basis of $\mathbb{L}'$ suffices.) The two definitions of $\mathcal{U}_P$ via lattices or isomorphisms with $\pi(\mathbb{L}) \subset \mathbb{L}$ are equivalent. We will use the common notation $\mathcal{U}_P$.

Example 2. Anisotropic dilatations. Take $\pi : \mathbb{Z}^n \to \mathbb{Z}^n$ defined by

$$\pi(x_1, \ldots, x_n) = (k_1 x_1, \ldots, k_n x_n),$$

where $k_1, \ldots, k_n \in \mathbb{N}$. The corresponding map $\mathcal{U}_P$ extends the notion of Ehrhart polynomial and Example 1.

Simple examples show that $\mathcal{U}_P$ is not a polynomial in the variables k_i.

2. A necessary condition

Given a nonzero $z \in \mathbb{L}^*$, the dual of $\mathbb{L}$, and an $\mathbb{L}$–polytope P, define $P(z)$ as the set of points in P where the functional z takes its maximal value. As is well known, $P(z)$ is a face of P. Denote by $H(z)$ the hyperplane $z \cdot x = 0$ (scalar product). $H(z)$ is clearly a lattice subspace.

Theorem 2. *Assume P, Q are $\mathbb{L}$–polytopes with identical universal counting function. Then, for every primitive $z \in \mathbb{L}^*$,*

$$(*) \qquad \operatorname{rvol} P(z) + \operatorname{rvol} P(-z) = \operatorname{rvol} Q(z) + \operatorname{rvol} Q(-z).$$

The theorem shows, in particular, that if $P(z)$ or $P(-z)$ is a facet of P, then $Q(z)$ or $Q(-z)$ is a facet of Q. Further, given an $\mathbb{L}$–polytope P, there are only finitely many possibilities for the outer normals and volumes of the facets of another polytope Q with $\mathcal{U}_P = \mathcal{U}_Q$. So a well–known theorem of Minkowski implies,

Corollary 1. *Assume P is an $\mathbb{L}$–polytope. Then, apart from lattice translates, there are only finitely many $\mathbb{L}$–polytopes with the same universal counting functions as P.*

Proof of Theorem 2. We assume that P, Q are full–dimensional polytopes. It is enough to prove the theorem in the special case when $\mathbb{L} = \mathbb{Z}^n$ and $z = (1, 0, \dots, 0)$. There is nothing to prove when none of $P(z), P(-z), Q(z)$, $Q(-z)$ is a facet since then both sides of (*) are equal to zero. So assume that, say, $P(z)$ is a facet, that is, $\operatorname{rvol} P(z) > 0$.

For a positive integer k define the linear map $\pi_k \colon V \to V$ by

$$\pi_k(x_1, \dots, x_n) = (x_1, kx_2, \dots, kx_n).$$

The condition implies that the lattice polytopes $\pi_k(P)$ and $\pi_k(Q)$ have the same Ehrhart polynomial. Comparing their second coefficients we get,

$$\sum_{F \text{ a facet of } P} \operatorname{rvol} \pi_k(F) = \sum_{G \text{ a facet of } Q} \operatorname{rvol} \pi_k(G),$$

since the facets of $\pi_k(P)$ are of the form $\pi_k(F)$ where F is a facet of P.

Let $\zeta = (\zeta_1, \dots, \zeta_n) \in \mathbb{Z}^{n*}$ be the (unique) primitive outer normal to the facet F of P. Then $\zeta' = (k\zeta_1, \zeta_2, \dots, \zeta_n)$ is an outer normal to $\pi_k(F)$, and so it is a positive integral multiple of the unique primitive outer normal ζ'', that is $\zeta' = m\zeta''$ with m a positive integer. When k is a large prime and ζ is different from z and $\zeta_1 \neq 0$, then $m = 1$ and $\operatorname{rvol} \pi_k(F) = O(k^{n-2})$. When $\zeta_1 = 0$, then $m = 1$, again, and the ordinary $(n-1)$–volume of $\pi_k(F)$ is $O(k^{n-2})$. Finally, when $\zeta = \pm z$, $\operatorname{Vol} \pi_k(F) = k^{n-1} \operatorname{Vol} F$.

So the dominant term, when $k \to \infty$, is $k^{n-1}(\operatorname{rvol} P(z) + \operatorname{rvol} P(-z))$ since by our assumption $\operatorname{rvol} P(z) > 0$. $\square$

3. Dimension two

Let P be an $\mathbb{L}$–polygon in V of dimension two. Simple examples show again that $\mathcal{U}_P$ is not a polynomial in the coefficients of π.

In the planar case we abbreviate $\operatorname{rvol} P(z)$ as $|P(z)|$. Extending (and specializing) Theorem 1 we prove

Proposition 3. *Suppose P and Q are $\mathbb{L}$–polygons. Then $\mathcal{U}_P = \mathcal{U}_Q$ if and only if the following two conditions are satisfied:*

(i) $\operatorname{Area}(P) = \operatorname{Area}(Q)$,

(ii) $|P(z)| + |P(-z)| = |Q(z)| + |Q(-z)|$ *for every primitive* $z \in \mathbb{L}^*$.

Proof. The conditions are sufficient: (i) and (ii) imply that, for any π, $\operatorname{Area}(\pi(P)) = \operatorname{Area}(\pi(Q))$ and $|\pi(P)(z)|+|\pi(P)(-z)| = |\pi(Q)(z)|+|\pi(Q)(-z)|$. We use Pick's formula for $\pi(P)$, (see [GW], say):

$$|\pi(P) \cup \mathbb{L}| = \operatorname{Area} \pi(P) + \frac{1}{2} \sum_{z \text{ primitive}} |\pi(P)(z)| + 1.$$

This shows that $\mathcal{U}_P = \mathcal{U}_Q$, indeed.

The necessity of (i) follows from Theorem 1 immediatley, (via the main coefficient of E_P), and the necessity of (ii) is the content of Theorem 2. $\square$

Corollary 2. *Under the conditions of Proposition 3 the lattice width of P and Q, in any direction $z \in \mathbb{L}^*$ are equal.*

Proof. The lattice width, $w(z, P)$, of P in direction $z \in \mathbb{L}^*$ is, by definition (see [KL],[Lo]),

$$w(z, P) = \max\{z \cdot (x - y) \colon x, y \in P\}.$$

In the plane one can compute the width along the boundary of P as well which gives

$$w(z, P) = \frac{1}{2} \sum_e |z \cdot e|$$

where the sum is taken over all edges e of P. This proves the corollary. $\square$

Theorem 3. *Suppose P and Q are $\mathbb{L}$–polygons. Then $\mathcal{U}_P = \mathcal{U}_Q$ if and only if the following two conditions are satisfied:*

(i) $\mathrm{Area}(P) = \mathrm{Area}(Q)$,

(ii) there exist $\mathbb{L}$–polygons X and Y such that P resp. Q is a lattice translate of $X + Y$ and $X - Y$ (Minkowski addition).

Remark. Here X or Y is allowed to be a segment or even a single point. In the proof we will ignore translates and simply write $P = X + Y$ and $Q = X - Y$.

Proof. Note that (ii) implies the second condition in Proposition 3. So we only have to show the necessity of (ii).

Assume the contrary and let P, Q be a counterexample to the statement with the smallest possible number of edges. We show first that for every (primitive) $z \in \mathbb{L}^*$ at least one of the sets $P(z), P(-z), Q(z), Q(-z)$ is a point.

If this were not the case, all four segments would contain a translated copy of the shortest among them, which, when translated to the origin, is of the form $[0, t]$. But then $P = P' + [0, t]$ and $Q = Q' + [0, t]$ with $\mathbb{L}$–polygons P', Q'.

We claim that P', Q' satisfy conditions (i) and (ii) of Proposition 3. This is obvious for (ii). For the areas we have that $\mathrm{Area}\, P - \mathrm{Area}\, P'$ equals the area of the parallelogram with base $[0, t]$ and height $w(z, P)$. The same applies to $\mathrm{Area}\, Q - \mathrm{Area}\, Q'$, but there the height is $w(z, Q)$. Then Corollary 2 implies the claim.

So the universal counting functions of P', Q' are identical. But the number of edges of P' and Q' is smaller than that of P and Q. Consequently there are polygons X', Y with $P' = X' + Y$, and $Q' = X' - Y$. But then, with $X = X' + [0, t]$, $P = X + Y$ and $Q = X - Y$, a contradiction.

Next, we define the polygons X, Y by specifying their edges. It is enough to specify the edges of X and Y that make up the edges $P(z), P(-z), Q(z), Q(-z)$ in $X+Y$ and $X-Y$. For this end we orient the edges of P and Q clockwise and set

$$P(z) = [a_1, a_2], P(-z) = [b_1, b_2], Q(z) = [c_1, c_2], Q(-z) = [d_1, d_2]$$

each of them in clockwise order. Then

$$a_2 - a_1 = \alpha t, b_2 - b_1 = \beta t, c_2 - c_1 = \gamma t, d_2 - d_1 = \delta t$$

where t is orthogonal to z and $\alpha, \gamma \geq 0$, $\beta, \delta \leq 0$ and one of them equals 0. Moreover, by condition (ii) of Proposition 3, $\alpha - \beta = \gamma - \delta$.

Here is the definition of the corresponding edges, x, y of X, Y:

$$\begin{aligned} x = \alpha t, y = \beta t &\text{ if } \delta = 0, \\ x = \beta t, y = \alpha t &\text{ if } \gamma = 0, \\ x = \gamma t, y = -\delta t &\text{ if } \beta = 0, \\ x = \delta t, y = -\gamma t &\text{ if } \alpha = 0. \end{aligned}$$

With this definition, $X+Y$ and $X-Y$ will have exactly the edges needed. We have to check yet that the sum of the X edges (and the Y edges) is zero, otherwise they won't make up a polygon. But $\sum(x+y) = 0$ since this is the sum of the edges of P, and $\sum(x-y) = 0$ since this is the sum of the edges of Q. Summing these two equations gives $\sum x = 0$, subtracting them yields $\sum y = 0$. $\square$

4. An example and a question

Let X, resp. Y be the triangle with vertices $(0,0), (2,0), (1,1)$, and $(0,0), (1,1), (0,3)$. As it turns out the areas of $P = X+Y$ and $Q = X-Y$ are equal. So Theorem 3 applies: $\mathcal{U}_P = \mathcal{U}_Q$. At the same time, P and Q are not congruent as P has six vertices while Q has only five.

However, it is still possible that polygons with the same universal counting function are equidecomposable. Precisely, $P_1, \ldots, P_m$ is said to be a subdivision of P if the P_i are $\mathbb{L}$–polygons with pairwise relative interior, their union is P, and the intersection of the closure of any two of them is a face of both. Recall from section 1 the group $\mathcal{G}_{tr}$ generated by $\mathbb{L}$–translations and the reflection with respect to the origin. Two $\mathbb{L}$–polygons P, Q are called $\mathcal{G}_{tr}$–equidecomposable if there are subdivisions $P = P_1 \cup \cdots \cup P_m$ and $Q = Q_1 \cup \cdots \cup Q_m$ such that each P_i is a translate, or the reflection of a translate of Q_i with the extra condition that P_i is contained in the boundary of P if and only if Q_i is contained in the boundary of Q.

We finish the paper with a question which has connections to a theorem of the late Peter Greenberg [Gr]. Assume P and Q have the same universal counting function. Is it true then that they are $\mathcal{G}_{tr}$–equidecomposable? In the example above, as in many other examples, they are.

References

[BK] U. Betke, M. Kneser, Zerlegungen und Bewertungen von Gitterpolytopen, *J. Reine ang. Math.* **358** (1985), 202–208.

[Eh] E. Ehrhart, *Polinomes arithmétiques et métode des polyédres en combinatoire*, Birkhauser, 1977.

[Gr] P. Greenberg, Piecewise SL_2–geometry, *Transactions of the AMS*, **335** (1993), 705–720.

[GW] P. Gritzmann, J. Wills, Lattice points, in: *Handbook of convex geometry, ed. P. M. Gruber, J. Wills*, North Holland, Amsterdam, 1988.

[KL] R. Kannan, L. Lovász, Covering minima and lattice point free convex bodies, *Annals of Math.* **128** (1988), 577–602.

[Ka] J–M. Kantor, Triangulations of integral polytopes and Ehrhart polynomials, *Beiträge zur Algebra und Geometrie*, **39** (1998), 205–218.

[Lo] L. Lovász, *An algorithmic theory of numbers, graphs and convexity*, Regional Conference Series in Applied Mathematics **50**, 1986.

[McM] P. McMullen, Valuations and dissections, in: *Handbook of convex geometry, ed. P. M. Gruber, J. Wills*, North Holland, Amsterdam, 1988.